UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/754,713	01/12/2004	Jason Whitman Keith Brothers	062070-0311769	1344

909 7590 03/26/2008

PILLSBURY WINTHROP SHAW PITTMAN, LLP
P.O. BOX 10500
MCLEAN, VA 22102

EXAMINER	
PALIWAL, YOGESH	
ART UNIT	PAPER NUMBER
2135	
MAIL DATE	DELIVERY MODE
03/26/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/754,713	KEITH BROTHERS ET AL.	
	Examiner	Art Unit	
	YOGESH PALIWAL	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE ____ MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *04 January 2008*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-31* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-31* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

- Applicant's submission for RCE filed on January 4, 2008 has been entered.
- Applicant has amended claims 1, 3, 6, 8, 10, 13, 16, 19, 21, 23, 27, 30, and 31. Currently claims 1-31 are pending in this application. Any well known art statements made in the prior office action not argued by applicant is taken as admittance of prior art as per MPEP 2144.03.
- Examiner acknowledges clarification of claim language of claims 3, 23, and 31 for minor informalities. As a result, all claim objections previously presented are withdrawn.
- Examiner acknowledges clarification of claim language of claim(s) 8 and 21 to overcome rejection under 35 U.S.C 112, first paragraph. As a result, all rejections under U.S.C 112, first paragraph previously presented are withdrawn.

Response to Arguments

1. Applicant's arguments filed 01/04/2008 have been fully considered but they are not persuasive for the following reasons:

- Regarding Claim 1, applicant argues, "Shetty specifically indicates that "protocol filters scan the traffic data stream for malwares" (col. 3, lines 17-20), distinguishing a "packet filter [that] looks at each packet entering or leaving the network and accepts or rejects it based on user-defined rules" (col. 5, lines 9-11). Thus, Shetty scans a data stream in a manner that depends on protocol information associated with the data stream, rather than packet information associated therewith. Accordingly, for at least this reason, Shetty does not disclose, teach, or suggest at least the feature of "monitoring the received packets to **identify one or more of the packets**

that include information associated with an attack signature, the attack signature associated with one or more previous attacks directed at the target system," as recited in claim 1, for example".

- Examiner respectfully disagrees with the applicant's interpretation of the Shetty reference. Applicant's cited part (Col. 5, lines 9-11) simply recites several types of firewall techniques that are known. Protocol information is only used to classify the incoming packet or stream of packets (see Col. 5, lines 21-45) and when packets are classified, each type of protocol scanner then examine the packet or packets within the stream of data using various function (see Column 3, line 56 through Column 4, line 13, describing various functions that the protocol scanner is capable of performing, including scanning for computer malwares, blocking an IP address or set of IP address, Blocking emails, Blocking ports and blocking URLs. Applicant should note that in order to perform blocking based on for example IP address of emails, scanner must identify these information within the packet prior to blocking that packet). Therefore, applicant argument that Shetty is only concerned with the protocol information is not found persuasive.

- Applicant further argues that, "Alampalayam fails to cure the aforementioned deficiencies of Shetty. Specifically, Alampalayam describes a "security model [that] uses feedback control scheme" in which "various parameters of an agent node or set of nodes are monitored. If these parameters change rapidly in a given time frame, appropriate threat is identified" (Section 2.2). As such, Alampalayam monitors network parameters, not "received packets," as recited in claim 1, for example. Moreover, Alampalayam identifies threats based on changes to values of the parameters, not based on "an attack signature . . . associated with one or more previous attacks directed at the target system," as recited in claim 1, for example. Accordingly, for at least these reasons, Alampalayam fails to cure the aforementioned deficiencies of Shetty."

- Examiner respectfully disagrees with the applicant's interpretation of the Alampalayam reference. Applicant admits that Alampalayam describes a security module that uses feedback control scheme in which various parameters of an agent node or set of nodes are monitored. Applicant further recite that Alampalayam monitors network parameters, not "received packet". Examiner disagrees and would like to point out that on page 1519, 1st column, 2nd paragraph, Alampalayam described these "network parameters" in details and recites, "Vulnerability level at each node can be computational matrices such as CPU time, number of existing services, buffer usage, power consumption, file system size etc., or **communicational metrics** such as bandwidth, interface speed, number of connection, service queue length, **packet drop rate, packets with error**, protocol (IP/ICMP/UDP/TCP) flow rate, number of collisions, connection utilization etc.". Therefore, Alampalayam monitors network parameter that includes monitoring information about received packet. Once the security module of Alampalayam detects an attack on the system, the protection framework then executes different security policy for the given scenario and thereby protects the network under a given situation (see Page 1519, 2nd Column, "Step 3: Protection Framework"). Therefore, contrary to applicant's assertion, examiner asserts that Alampalayam discloses the amended claim limitation of "attack signature associated with one or more previous attacks directed at the target system".

Claim Rejections - 35 USC § 103

2. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a

whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1, 2, 3, 4, 5, 6, 7, 8, 10, 12, 13, 14, 16, 17, 18, 19, 20, 21, 23, 25, 26, 27, 28, 30, 31 are rejected under 35 U.S.C. 103(a) as being unpatentable over Shetty (US 6,772,345), hereinafter Shetty, in view of Alampalayam et al. (Alampalayam, S.P.; Anup Kumar, "An adaptive security model for mobile agents in wireless networks," Global Telecommunications Conference, 2003. GLOBECOM '03. IEEE , vol.3, no., pp. 1516-1521 vol.3, 1-5 Dec. 2003), hereinafter Alampalayam.

Regarding **Claims 1, 10 and 16**, Shetty discloses a method, system and computer program product for detecting and preventing attacks directed at a target system (Column 1, lines 6-8, "The present invention relates to a method, system and computer program product for detecting computer malwares that scans network traffic at the protocol level"), comprising:

receiving one or more packets originating from a source system (Fig. 1, Numeral 102, "Network Traffic In"), the received packets directed to the target system (Fig. 1, numeral 104, "Network Traffic Out" and also at Column 1, lines 58-60, "Malware scanning of data that is being transferred or downloaded to a computer system");

monitoring the received packets to identify one or more of the packets that include information associated with a signature of an attack directed at the target system (Column 1, lines 65-66, "Scanning the data stream at a protocol level to detect a malware", also see Column 3, line 56 through Column 4, line 13, describing various functions that the protocol scanner is capable of performing, including scanning for computer malwares, blocking an IP address or set of IP address, Blocking emails, Blocking ports and blocking URLs. Applicant should note that in order to perform blocking based on for example IP address of emails, scanner must identify these information within the packet prior to blocking that packet);

Shetty discloses identifying packets that includes information associated with an attack signature, however, Shetty does not explicitly discloses that the attack signature associated with one or more previous attacks directed at the target system. In other words, Shetty lacks adaptive signature creating technique.

Alampalayam discloses adaptive security model that uses feedback technology to first detect an attack on the network and then based on the attack it creates a signature associated with that attack to block the current and future data from the attacking source (see Page 1519, 2nd Column, Step 3: Protection Framework, "Based on the security level input received from the error detection framework, the protection framework would execute different security policy for the given scenario and thereby protecting the network under a given situation.")

Therefore, it would have been obvious at the time the invention was made to one of ordinary skill in the art to add into a protocol filter of Shetty, a feedback technology for dynamic policy or signature creation as taught by Alampalayam discloses a scheme that provides a security framework that will detect automatically various attacks and then take appropriate measures to deal with the attack (see Alampalayam, Abstract). Furthermore, the protocol filter of Shetty is capable of blocking packet from specific IP addresses (See, Shetty, Column 3, lines 61-64) but Shetty does not explicitly discloses that this list of IP address can be updated based on new attacks on the system. However, Alampalayam discloses blocking an IP address when DOS attack is detected (see Page 1519, 2nd Column, "Step 3: Protection Framework"). Therefore, the combined system of Shetty and Alampalayam would then not only block the IP address that Shetty has pre-defined but would also be able to add more IP address dynamically after the detection of a DOS attack as taught by Alampalayam and thus combining Alampalayam with Shetty would increase the overall security of the Shetty's protocol scanner.

The combined system of Shetty and Alampalayam further discloses:

detecting an attack directed at the target system when one or more of the monitored packets include information associated with the attack signature (see Shetty, Column 3, line 56 through Column 4, line 13, describing various functions that the protocol scanner is capable of performing, including scanning for computer malwares, blocking an IP address or set of IP address, Blocking emails, Blocking ports and blocking URLs. Applicant should note that in order to perform blocking based on for example IP address of emails, scanner must identify these information within the packet prior to blocking that packet, also see Alampalayam, Page 1519, 2nd Column, "Step 3: Protection Framework")

blocking the identified packets that includes information associated with the attack signature from being transmitted to the target system (see Shetty, Column 5, lines 5-8 "All messages entering or leaving the intranet pass through the firewall, which examines each message and blocks those that do not meet the specified security criteria", also see Column 3, line 56 through Column 4, line 13); and

blocking one or more subsequently received packets from being transmitted to the target system when a severity of the detected attack exceeds a predetermined threshold, and the subsequently blocked packets including one or more of packets originating from the source system or directed to the target system (see, Alampalayam, Page 1519, 2nd Column, "Step 3: Protection Framework" section, "For instance, once a DoS attack is detected, security level is increased. This causes the malicious nodes causing DoS attack to be disconnected or specific mobile IP address is blocked/automatically denied future connections from accessing the network.")

Regarding **Claims 2 and 12**, the rejection of claims 1 and 10 is incorporated and Shetty further discloses that monitoring the data packets includes determining at least one of identifying information or a type of communication associated with the monitored packets (Column 3 lines 13-17, "As shown in FIG. 1,

incoming network traffic 102 and outgoing network traffic 104 are filtered by one or more protocol filters, such as filters 106A-C. The protocol filters scan the traffic data stream for malwares").

Regarding **Clam 3**, the rejection of claim 2 is incorporated and further Shetty discloses wherein the identifying information includes at least one of a source Internet Protocol Address, a source port number, a destination Internet Protocol address, or a destination port number (Column 3, lines 56-57,61 and Column 4 line 1, "Preferably, protocol scanner 108 will be capable of performing a number of function:" … "Blocking an IP address or set of IP address" … "Blocking ports") *[Shetty's system is capable of blocking incoming packets based on the source IP address or just block traffic on certain ports]*

Regarding **Claim 31**, the rejection of claim 3 is incorporated and the combination of Shetty and Alampalayam further discloses that the subsequently blocked packets including packets associated with one or more of the source Internet Protocol address, the source port number, the destination Internet Protocol address, or the destination port number (Page 1519, 2nd Column, "Step 3: Protection Framework" section, "For instance, once a DoS attack is detected, security level is increased. This causes the malicious nodes causing DoS attack to be disconnected or specific mobile IP address is blocked/automatically denied future connections from accessing the network.").

Regarding **Claim 4**, the rejection of claim 2 is incorporated and further Shetty discloses that the type of communication includes at least one of File Transfer Protocol, Simple Mail Transfer Protocol, Telnet, Domain Name System, Windows Internet Name System, HyperText Transfer Protocol, Traceroute, instant messaging, or chat (Column 3, lines 21-28, "Filter functionality is required for each protocol that is to be supported. For example, Post Office Protocol 3 (POP3) filter 106A scans the POP3 data stream, HyperText Transfer Protocol (HTTP) filter 106B scans the HTTP data stream, and File Transfer Protocol (FTP) filter 106C scans the FTP data stream. POP3 is a protocol used to retrieve e-mail from a mail server,

HTTP is the underlying protocol used by the World Wide Web, and FTP is a protocol used on the Internet for sending files")

Regarding **Claim 5**, the rejection of claim 1 is incorporated and Shetty further discloses that monitoring the packets includes using Transmission Control Protocol/Internet Protocol at an application layer (Column 3, lines 58-60, "Scanning for computer malwares, such as viruses, Trojans and worms in the entire network TCP/IP protocol like HTTP, FTP, SMTP/POP3, etc.")

Regarding **Claims 6, 13 and 19**, the rejection of claims 1, 10 and 16 is incorporated and Alampalayam further discloses that the severity of the detected attack is determined based on at least one of a frequency of previous attacks, a type of communication used in the previous attacks, an amount of bandwidth usage associated with the previous attack, or a volume of received data packets (see, page 1519, 1st column, 2nd paragraph, "Vulnerability level at each node can be computational matrices such as CPU time, number of existing services, buffer usage, power consumption, file system size etc., or communicational metrics such as bandwidth, interface speed, number of connection, service queue length, packet drop rate, packets with error, protocol (IP/ICMP/UDP/TCP) flow rate, number of collisions, connection utilization etc.")

Regarding **Claims 7, 14, and 20**, the rejection of claims 1, 10 and 16 is incorporated and Shetty further discloses wherein blocking the data packets from being transmitted to the target system includes instructing at least one of a router, a hub, a server, or a firewall to disable a communication channel. (Column 5, lines 5-8 "All messages entering or leaving the intranet pass through the firewall, which examines each message and blocks those that do not meet the specified security criteria")

Regarding **Claim 17**, the rejection of claim 16 is incorporated and Shetty further discloses that the that the received packets are monitored transparently in real-time (Column 1, lines 58-60, "Malware

scanning of data that is being transferred or downloaded to a computer system") [It can be seen that security configuration of Shetty's system that includes router/firewall and gateway system that is responsible for scanning incoming data is transparent to both the data receiving and sending host]

Regarding **Claim 18**, the rejection of claim 16 is incorporated and further Shetty discloses that the received packets are monitored after being stored in a storage buffer (Column 7, lines 22-27, "Memory 408 includes protocol scanner 410, which includes at least one protocol filter, such as protocol filters 412A and 412B, application programs 414, and operating system 412. Protocol scanner 410 scans for network traffic for malwares and then forwards the scanned data to workstation computers and/or workstation computer applications")

Regarding **Claim 23**, Shetty discloses a computer system configured for detecting and preventing attacks directed at target device (Column 1, lines 6-8, "The present invention relates to a method, system and computer program product for detecting computer malwares that scans network traffic at the protocol level"), comprising:

at least one terminal device (Figure 3, Numeral 312A, "WORKSTATION");

at least one server (Figure 3, Numeral 310, "PROTOCOL SCANNER") coupled to a computer network (Fig. 3, Numeral 302, "Network") and to the terminal device (Fig. 3, Numeral 312A, "Workstation"), the server operable to monitor packets directed to the terminal device, the server having one or more modules (It is implied that firewall contains software modules that does the scanning of incoming packets) including:

Other limitations of this claim are similar to claim 10 and the combination of Shetty and Alampalayam discloses the remaining limitations (see rejection of claim 10 above).

Regarding **Claim 25**, the rejection of claim 23 is incorporated and further Shetty discloses a database coupled to the server (Column 3, lines 61-67 and Column 4, lines 1-13) [Since the protocol scanner is capable of blocking data based on IP address or specific e-mail address, specific block and specific URLs, then it must have a database with all the entries of the IP addresses, e-mail address, port numbers and URLs to block]

Regarding **Claim 26**, the rejection of claim 23 is incorporated and further Shetty discloses that the detection module monitors the received packets by determining at least one of identifying information or a type of communication associated with the monitored packets. (Column 3 lines 13-17, "As shown in FIG. 1, incoming network traffic 102 and outgoing network traffic 104 are filtered by one or more protocol filters, such as filters 106A-C. The protocol filters scan the traffic data stream for malwares").

Regarding **Claim 27**, the rejection of claim 23 is incorporated and Alampalayam further discloses that the severity of the detected attack is determined based on at least one of a frequency of previous attacks, a type of communication used in the previous attacks, an amount of bandwidth usage associated with the previous attack, or a volume of received data packets (see, page 1519, 1st column, 2nd paragraph, "Vulnerability level at each node can be computational matrices such as CPU time, number of existing services, buffer usage, power consumption, file system size etc., or communicational metrics such as bandwidth, interface speed, number of connection, service queue length, packet drop rate, packets with error, protocol (IP/ICMP/UDP/TCP) flow rate, number of collisions, connection utilization etc.")

Regarding **Claim 28**, the rejection of claim 23 is incorporated and Shetty further discloses that the blocking module blocks data packets from being transmitted to the terminal device by instructing at least one of a router, a hub, a server, or a firewall to disable a communication channel (Column 5, lines 5-8 "All

messages entering or leaving the intranet pass through the firewall, which examines each message and blocks those that do not meet the specified security criteria").

Regarding **Claims 8, 21 and 30**, the rejection of claims 1, 16 and 23 is incorporated and the combination of Shetty and Alampalayam further discloses notifying the source system that the attack has been detected and that a block was placed on packets received from the source system (see Alampalayam, Page 1519, "Step 3: Protection Framework" section, "If one require a message to be sent back to node (agent), the redirection feature would be used instead of deny feature, to redirect specific document to specific node (agent)".

Claims 9, 11, 15, 22, 24 and 29 are rejected under 35 U.S.C. 103(a) as being unpatentable over Shetty in view of Alampalayam and further in view of Lachman, III et al. (US 2002/0166063).

Regarding **Claims 9, 15, 22 and 29**, rejections of claims 1, 14, 16, and 23 are incorporated and the combination of Shetty and Alampalayam teaches blocking data packets. The combination does not teach that the subsequently received packet are blocked from being transmitted to the target system for a predetermine amount of time.

However, Lachman, III et al., in the same field of endeavor of network security, discloses the data packets are blocked from entering the target system for a predetermined amount of time (Paragraph 0125, "If the flooding is of the single-source type, no packets will be routed from that source to the victim IP address for the specified block time).

Therefore, it would have been obvious at the time the invention was made to one of ordinary skill in the art to block the data packets as disclosed by Shetty for only a predetermined amount of time as taught by Lachman, III et al. to *"prevent network flood interruptions without disrupting normal network operations" (Paragraph 0002, Lachman, III et al.)*

Regarding **Claims 11 and 24**, rejections of claims 10 and 23 are incorporated and the combination of Shetty and Alampalayam doesn't disclose a log of the packets identified as including the information associated with the attack signatures.

However, Lachman, III et al. further discloses a log-creating module that is adapted to create a log of the received data packets having the attack signatures **(Paragraph 0105, "if the network load reaches the set threshold, then system 106 can launch a countermeasure routine and can log the time of the flood, the time of the countermeasure deployment, and the source and destination of the offending packet (s).")**

Therefore, it would have been obvious at the time the invention was made to one of ordinary skill in the art to create a log, as taught by Lachman, III et al., of the received data packets having the attack signature in the system of Shetty so that *the source of the offending packet* ***(Lachman, III et al., Paragraph 0105)*** *can be added to the blocking list of Shetty's router/firewall so that "the source will not [be] able to send or receive any data from the protected corporation network"* ***(Shetty, Column 3, lines 62-64).***

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to YOGESH PALIWAL whose telephone number is (571)270-1807. The examiner can normally be reached on M-F: 7:30 AM - 5:00 PM EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on (571) 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Y. P./
Examiner, Art Unit 2135
/KIMYEN VU/
Supervisory Patent Examiner, Art Unit 2135